PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer: WO 99/33270
H04N 7/167, H04L 9/08	A1	(43) Internationales Veröffentlichungsdatum: 1. Juli 1999 (01.07.99)

(21) Internationales Aktenzeichen: PCT/EP97/07124

(22) Internationales Anmeldedatum: 18. Dezember 1997 (18.12.97)

(71) Anmelder: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder: SCHWENK, Jörg; Südwestring 27, D–64807 Dieburg (DE).

(81) Bestimmungsstaaten: CA, CN, JP, KR, TR, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: METHOD FOR SECURING A SYSTEM PROTECTED BY KEY HIERARCHY

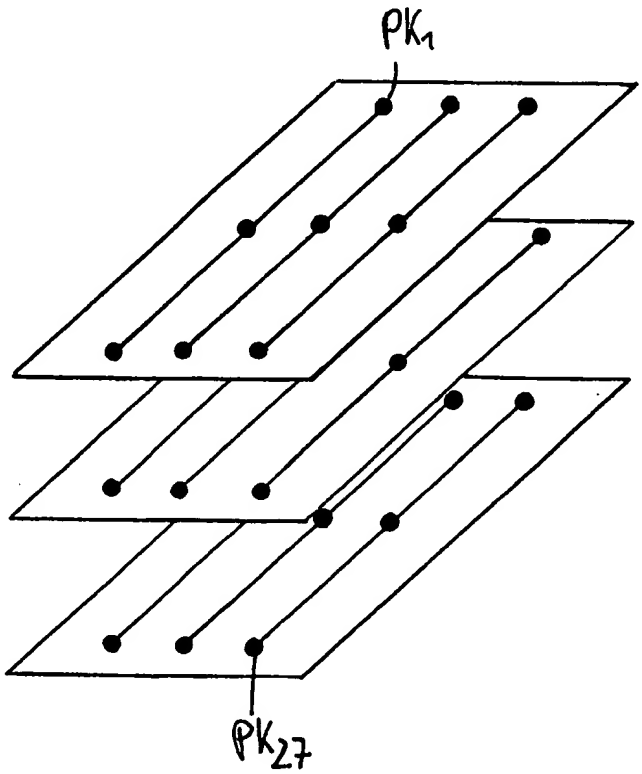
(54) Bezeichnung: VERFAHREN ZUM SICHERN EINES DURCH EINE SCHLÜSSELHIERARCHIE GESCHÜTZTEN SYSTEMS

(57) Abstract

The invention relates to a method for securing at least one system protected by a predetermined hierarchy of cryptographic keys, more particularly a Pay–TV system, against unauthorized users. Current key hierarchy systems do not enable detection of unreliable clients who make copies of a group key transmitted by a system provider and pass them on to other persons. According to the invention, this is solved by detecting at least one individual cryptographic key assigned to an unreliable user by forming the intersection of at least two predetermined subsets formed at different times and belonging to the same hierarchy.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zum Sichern wenigstens eines durch eine vorbestimmte Hierarchie von kryptografischen Schlüsseln geschützten Systems, insbesondere eines Pay–TV–Systems, gegen unberechtigte Nutzer. In Schlüsselhierarchie–Systemen gibt es derzeit keine Möglichkeit, einen unzuverlässigen Kunden zu ermitteln, der einen vom Systembetreiber übermittelten Gruppenschlüssel kopiert und an beliebige Personen weiterveräußert hat. Die Erfindung schlägt als Lösung vor, daß wenigstens ein einem unzuverlässigen Nutzer zugeordneter, individueller kryptografischer Schlüssel ermittelt wird, indem die Schnittmenge von wenigstens zwei vorbestimmten, zu verschiedenen Zeitpunkten gebildeten Teilmengen, die der gleichen Hierarchieebene angehören, gebildet wird.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verfahren zum Sichern eines durch eine Schlüsselhierarchie geschützten Systems

Die Erfindung betrifft ein Verfahren zum Sichern wenigstens eines durch eine vorbestimmte Hierarchie von kryptografischen Schlüsseln geschützten Systems, insbesondere eines Pay-TV-Systems, gegen unberechtigte Nutzer gemäß Anspruch 1.

Auf vielen Einsatzgebieten wird eine Schlüsselhierarchie verwendet, um aus den individuellen kryptografischen Schlüsseln der Kunden einen für eine große Anzahl von Kunden gemeinsamen Schlüssel abzuleiten. Einen typischen Anwendungsfall stellt ein Pay-TV-System dar. Mit Hilfe einer Schlüsselhierarchie ist es möglich, die Erlaubnis zum Empfang eines Pay-TV-Programms selektiv nur an ausgewählte Kunden zu verteilen. Eine mögliche Schlüsselhierarchie weist die Form einer Baumstruktur auf. In der untersten Hierarchieebene erhält jeder potentielle Kunde zunächst eine Chipkarte oder ein anderes Sicherheitsmodul, auf der ein individueller, eindeutig dem Kunden zugeordneter Schlüssel gespeichert ist. Der Pay-TV-Programmanbieter speichert alle diese individuellen kryptografischen Schlüssel in einer zentralen Speichereinrichtung. Stufenweise wird danach die Schlüsselhierarchie aufgebaut, indem in der zweiten Ebene zunächst die Schlüssel der untersten Ebene zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt werden. Jeder Teilmenge wird ein kryptografischer Gruppenschlüssel zugeordnet, der mit Hilfe der die kryptografischen Schlüssel der untersten Ebene, die die jeweilige Teilmenge bilden, übermittelt wird. Anschließend werden in der dritten Ebene die Teilmengen der zweiten Ebene zu mehreren Teilmengen zusammengefaßt, wobei jede Teilmenge der dritten Ebene größer ist als jede Teilmenge der zweiten Ebene. Jeder Teilmenge der dritten Ebene wird ein kryptografischer

Gruppenschlüssel zugeordnet, der mit Hilfe der kryptografischen Gruppenschlüssel der zweiten Ebene, die die jeweilige Teilmenge bilden, übermittelt wird. Dieses Verfahren kann solange fortgesetzt werden, bis ein gemeinsamer Schlüssel für die Kunden, die zum Empfang des Pay-TV-Programms berechtigt sind, generiert ist. Auf ein solches, durch eine Schlüsselhierarchie geschütztes System sind verschiedene Angriffe denkbar, die alle davon ausgehen, daß ein unzuverlässiger Kunde den individuellen Schlüssel, einen oder mehrere Gruppenschlüssel oder den gemeinsamen Schlüssel, die auf seiner oder einer anderen Chipkarte gespeichert sind, kennt und diese unberechtigterweise an beliebige Dritte weitergibt. Man unterscheidet drei mögliche Angriffe auf ein solches System:

1. Der unzuverlässige Kunde kopiert den gemeinsamen Schlüssel und gibt diesen unberechtigterweise, z.B. auf einer Piratenchipkarte, an andere Personen weiter. Dieser Angriff kann dadurch abgewehrt werden, daß der Systembetreiber, der die kryptografischen Schlüssel generiert, den gemeinsamen Schlüssel in entsprechend kurz gewählten Zeitintervallen neu generiert.

2. Ein unzuverlässiger Kunde kopiert seinen individuellen kryptografischen Schlüssel und gibt diesen unberechtigterweise an andere Personen weiter. In diesem Fall kann der Kunde relativ einfach von der Nutzung des Systems ausgeschlossen werden, wenn der kopierte individuelle Schlüssel, z.B. auf einer Piratenkarte, erkannt wird. Denn zwischen dem individuellen kryptografischen Schlüssel und der dazugehörigen Person besteht ein eindeutiger Zusammenhang.

3. Ein unzuverlässiger Kunde kopiert einen Gruppenschlüssel und gibt diesen weiter. In diesem Fall ist es ohne weiteres nicht möglich, den unzuverlässigen Kunden eindeutig anhand des kopierten Gruppenschlüssels zu

identifizieren. Der Systembetreiber muß entweder alle Kunden der durch den Gruppenschlüssel identifizierten Gruppe von der Benutzung des Systems ausschließen oder den Mißbrauch durch den kopierten Gruppenschlüssel tolerieren.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren bereitzustellen, mit dem ein durch eine Schlüsselhierarchie geschütztes System gegen unberechtigte Nutzer effektiver geschützt werden kann.

Dieses technische Problem löst die Erfindung mit den Verfahrensschritten des Anspruchs 1.

Jedem potentiellen Systemnutzer wird in der untersten Ebene der Schlüsselhierarchie ein individueller kryptografischer Schlüssel zugeordnet, der ihm beispielsweise durch eine Chipkarte oder ein anderes Sicherheitsmodul ausgehändigt werden kann. Die individuellen kryptografischen Schlüssel jedes Nutzers werden in einer dem System zugeordneten Speichereinrichtung abgespeichert. Zu vorbestimmten diskreten Zeitpunkten wird anschließend wenigstens eine höhere Hierarchieebene von kryptografischen Schlüsseln durch folgende Schritte gebildet: die kryptografischen Schlüssel der unmittelbar niedrigeren Hierarchieebene werden in beliebiger Weise zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt, wobei jeder Teilmenge ein kryptografischer Schlüssel zugeordnet wird, der mit Hilfe der die jeweilige Teilmenge bildenden kryptografischen Schlüssel übermittelt und anschließend in der Speichereinrichtung abgelegt wird. Danach wird wenigstens ein einem verdächtigen Nutzer zugeordneter individueller kryptografischer Schlüssel ermittelt, indem die Schnittmenge von wenigstens zwei vorbestimmten, zu verschiedenen Zeitpunkten gebildeten Teilmengen, die der gleichen Hierarchieebene angehören, gebildet wird.

Vorteilhafte Weiterbildungen sind in den Unteransprüchen angegeben.

Statt zu vorbestimmten diskreten Zeitpunkten die höheren Hierarchieebenen neu zu bilden, können für unterschiedliche Systembetreiber gleichzeitig verschiedene Schlüsselhierarchien erzeugt werden. Jede Schlüsselhierarchie weist wenigstens eine höhere Hierarchieebene von kryptografischen Schlüsseln auf. Eine höhere Hierarchieebene wird dadurch gebildet, daß die kryptografischen Schlüssel der unmittelbar niedrigeren Hierarchieebene in beliebiger Weise zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt werden, wobei jeder Teilmenge ein kryptografischer Schlüssel zugeordnet wird, der aus den die jeweilige Teilmenge bildenden kryptografischen Schlüssel generiert und anschließend in der Speichereinrichtung abgelegt wird. Danach wird wenigstens ein einem verdächtigen Nutzer zugeordneter individueller kryptografischer Schlüssel ermittelt, indem die Schnittmenge von wenigstens zwei vorbestimmten Teilmengen, die der gleichen Hierarchieebene verschiedener Schlüsselhierarchien angehören, gebildet wird.

Man kann zur Realisierung dieses Verfahrens sukzessive immer größere Teilmengen entsprechend der Anzahl von Hierarchieebenen bilden. Ein mögliches Beispiel hierfür wäre eine Schlüsselhierarchie in Baumstruktur. Eine besonders effiziente Lösung ergibt sich jedoch, wenn man geometrische Strukturen verwendet, um die kryptografischen Schlüssel zu Teilmengen vorbestimmter Größe zusammenzufassen. Geometrische Strukturen bieten den Vorteil, daß die Eigenschaften der Schnittmengenbildung verschiedener Teilmengen sehr gut beschrieben werden können.

Vorzugsweise kann eine für mehrere Kunden erzeugte Schlüsselhierarchie mit Hilfe eines endlichen affinen Raums AG(d, q) der Dimension d über dem Körper GF(q) realisiert

werden (siehe A. Beutelspacher, Einführung in die endliche Geometrie I & II, BI Wissenschaftsverlag 1982, und A. Beutelspacher und U. Rosenbaum, Projektive Geometrie, Vieweg Verlag, 1992).

Die Schnittmengenbildung wird noch einfacher, wenn die geometrische Struktur ein endlicher projektiver Raum PG(d, q) der Dimension d über dem Körper GF(q) ist.

Die Erfindung wird nachfolgend anhand mehrerer Ausführungsbeispiel in Verbindung mit den beiliegenden Zeichnungen näher erläutert. Es zeigen:

Fig. 1 eine Schlüsselhierarchie für vier berechtigte Teilnehmer in Baumstruktur, die zu einem ersten Zeitpunkt gebildet worden ist,

Fig. 2 eine Schlüsselhierarchie nach Fig. 1, die jedoch zu einem zweiten Zeitpunkt generiert worden ist,

Fig. 3 eine Schlüsselhierarchie für 27 Teilnehmer des affinen Raums AG(3,3), die zu einem ersten Zeitpunkt gebildet worden ist,

Fig. 4 eine Schlüsselhierarchie nach Fig. 3, die zu einem zweiten Zeitpunkt erzeugt worden ist, und

Fig. 5 zwei verschiedene, zur gleichen Zeit existierende Schlüsselhierarchien.

In Fig. 1 ist eine Schlüsselhierarchie in Baumstruktur beispielsweise für ein Pay-TV-System dargestellt, das beispielsweise fünf Kunden umfaßt. Jeder Kunde i erhält von einem Sytembetreiber oder Pay-TV-Programmanbieter einen individuellen kryptografischen Schlüssel PK_i, der in der untersten Hierarchieebene angeordnet wird. Die unterste Hierarchieebene enthält somit fünf individuelle kryptografische Schlüssel PK_1-PK_5. Der Anbieter speichert diese Schlüssel in einer zentralen Speichereinrichtung. Mit Hilfe der verwendeten Baumstruktur ist es nunmehr möglich, ausgewählten Kunden die Erlaubnis zum Empfang eines Pay-TV-

Programms einzuräumen. Beispielsweise sollen nur die Kunden 1, 2, 3, und 4 zum Empfang des TV-Programms autorisiert werden, der Kunde 5 dagegen nicht. Um diese Berechtigungszuweisung zu erreichen, werden die Kunden 1 bis 4 in der nächsthöheren Hierarchieebene - das ist die zweite Ebene - vorteilhafterweise zu zwei Teilmengen mit jeweils zwei Kunden zusammengefaßt. In der Praxis geschieht dies dadurch, daß in einer zentralen Stelle zunächst für die beiden Teilmengen jeweils ein Gruppenschlüssel GK_1 bzw. GK_2 generiert wird. Der Gruppenschlüssel GK_1 wird mit Hilfe der beiden individuellen kryptografischen Schlüssel PK_1 und PK_2 der Kunden 1 bzw. 2 übertragen, wohingegen der Gruppenschlüssel GK_2 mit Hilfe der beiden individuellen kryptografischen Schlüsseln PK_3 und PK_4 der Kunden 3 bzw. 4 übertragen wird. Die Kunden 1 und 2 können mittels ihres individuellen kryptografischen Schlüssel PK_1 bzw. PK_2 den Gruppenschlüssel GK_1 berechnen, wohingegen die Kunden 3 und 4 mittels ihrer individuellen kryptografischen Schlüssel PK_3 bzw. PK_4 den Gruppenschlüssel GK_2 berechnen können. Der Kunde 5 hingegen kann keinen der beiden Gruppenschlüssel entschlüsseln. In der höchsten Hierarchieebene - das ist hier die dritte Ebene - wird danach eine Gesamtmenge gebildet, die die beiden Teilmengen der unmittelbar darunterliegenden Ebene 2 und damit die vier berechtigten Kunden enthält. In der zentralen Stelle wird dazu ein gemeinsamer Schlüssel SK mit Hilfe der beiden Gruppenschlüssel GK_1 und GK_2 der zweiten Ebene übertragen. Da das vom Anbieter ausgestrahlte Pay-TV-Programm mit dem gemeinsamen Schlüssel SK verschlüsselt ist, können die Kunden 1 bis 4 das Programm entschlüsseln und empfangen, der Kunde 5 hingegen nicht. Die in Fig. 1 dargestellte Schlüsselhierarchie umfaßt beispielhaft drei Hierarchieebenen.

Die Erfindung beschäftigt sich nunmehr mit dem Problem, einen unzuverlässigen Kunden ausfindig zu machen, der einen Gruppenschlüssel GK_1 oder GK_2 kopiert und unberechtigterweise

an Dritte weitervertreiben hat. Der unzuverlässige Kunde kann die "gestohlenen" Gruppenschlüssel in Form von Piraten-Chipkarten veräußern oder auch unter einer e-Mail-Adresse anbieten. Es sei angenommen, daß es sich bei dem Kunden 4 um den unzuverlässigen Kunden, nachfolgend auch Pirat genannt, handelt, der den Gruppenschlüssel $GK_{2,}$, der von der zentralen Stelle zuvor rundgesendet worden ist, kopiert und nun an beliebige Dritte weiterveräußert hat. Wenn der Systembetreiber in den Besitz des kopierten Gruppenschlüssels GK_2 kommt, kann er den Piraten nicht eindeutig ermitteln, da der Gruppenschlüssel GK_2 den beiden Kunden 3 und 4 zugeordnet ist. Es ist nun Ziel der Erfindung, den unzuverlässigen Kunden 4 aus der Gruppe von Kunden herauszufinden, die durch den Gruppenschlüssel GK_2 identifiziert sind. Dazu wird die verdächtige Gruppe mit ihrem zugeordneten kryptografischen Schlüssel GK_2 in der zentralen Stelle abgespeichert. Zu einem vorbestimmten Zeitpunkt generiert die zentrale Stelle eine neue Schlüsselhierarchie, die in Fig. 2 dargestellt ist. gebildet. Dazu werden willkürlich zwei neue Teilmengen gebildet, die beispielsweise die Kunden 1, 3 bzw. 2 und 4 umfassen. Die Neubildung der Teilmengen wird in der zentralen Stelle verwirklicht, indem für jede Teilmenge ein neuer Gruppenschlüssel GK_1' bzw. GK_2' generiert wird. Darüber hinaus wird auch ein neuer gemeinsamer Schlüssel SK' erzeugt. Die Vorgehensweise zur Erzeugung von Gruppenschlüssel und eines gemeinsamen Schlüssels wurde bereits oben ausführlich erläutert. Die neu generierten kryptografischen Schlüssel werden wiederum zu den einzelnen Kunden ausgesendet und in der zentralen Stelle abgespeichert. Der Pirat, in unserem Fall der Kunde 4, ist nunmehr gezwungen, den neuen Gruppenschlüssel GK_2' zu kopieren und an beliebige Personen zu verteilen. Sobald die zentrale Stelle im Besitz des kopierten Gruppenschlüssels GK_2' ist, wird dieser in der zentralen Speichereinrichtung abgespeichert. Anschließend wird die Schnittmenge aus der Teilmenge, der der kryptografische Gruppenschlüssel GK_2

zugeordnet ist, und der Teilmenge, der der kryptografische Gruppenschlüssel GK_2' zugeordnet ist, ermittelt. Da die zum ersten Zeitpunkt (s. Fig. 1) gebildete Teilmenge die Kunden 3 und 4 und die zum zweiten Zeitpunkt (s. Fig. 2) gebildete Teilmenge die Kunden 2 und 4 enthält, ergibt sich als Schnittmenge der Kunde 4. Die zentrale Stelle kennt nun den unzuverlässigen Kunden und kann ihn von der Nutzung des Systems ausschließen, indem beispielsweise sein individueller kryptografischer Schlüssel PK_4 gesperrt wird.

Obwohl die in Fig. 1 und 2 gezeigten Schlüsselhierarchien nur vier Kunden erfassen, können Schlüsselhierarchien beliebiger Größe verwendet werden. Damit erhöht sich selbstverständlich auch der Aufwand, einen unzuverlässigen Kunden zu finden, da die Anzahl der Gruppen größer ist.

In Fig. 3 und 4 sind zwei zu unterschiedlichen Zeitpunkten gebildete Hierarchien von Teilmengen beschrieben, die mit Hilfe des endlichen affinen Raums AG(3,3) der Dimension 3 über den Körper GF(3) realisiert werden können. Der in Fig. 3 und 4 dargestellte affine Raum besteht aus 27 Punkten, die den potentiellen Pay-TV-Kunden entsprechen. Es ist vorteilhaft, die Hierarchie von Teilmengen mit Hilfe des endlichen affinen Raums zu realisieren, da damit die Eigenschaften der Schnittmengenbildung verschiedener Teilmengen sehr genau beschrieben werden kann. Fig. 3 zeigt die zu einem ersten Zeitpunkt gebildete Hierarchie. Jedem Kunden wird wieder ein individueller kryptografischer Schlüssel PK_1 bis PK_{27} bereitgestellt. Man kann sich nun vorstellen, daß jedem Punkt des affinen Raums ein kryptografischer Schlüssel des jeweiligen Kunden zugeordnet ist. Die 27 Punkte können sukzessive zu Teilmengen von drei bzw. neun Punkten zusammengefaßt werden, indem man zunächst neun parallele Geraden auswählt und danach drei parallele Ebenen, die mit den Geraden verträglich sein müssen. Mit anderen Worten müssen die Geraden jeweils vollständig in einer der drei Ebenen enthalten sein. Übertragt man diese Struktur auf eine Schlüsselhierarchie, liegen die einzelnen Punkte in der untersten Ebene, die Geraden in der zweiten

Ebene, die drei Ebenen des affinen Raumes in der dritten Ebene, wobei die höchste Hierarchieebene den gesamten, die einzelnen Punkte, die neun Geraden und drei Ebenen umfassenden Raum enthält. In der zentralen Stelle werden nach dem bereits ausführlich beschriebenen Verfahren für jede Gerade, für jede Ebene des affinen Raums Gruppenschlüssel und für den Raum selbst ein gemeinsamer, alle Kunden umfassender Schlüssel generiert. Der Vorteil der geometrischen Strukturen und insbesondere von affinen Räumen besteht nun darin, daß man genau angeben kann, wieviele Teilmengen (Geraden oder Ebenen) man kennen muß, um einen bestimmten Punkt zu ermitteln. So schneiden sich beispielsweise zwei nichtparallele Ebenen eines affinen Raums genau in einer Geraden, und drei paarweise nichtparallele Ebenen in genau einem Punkt. Um beispielsweise den individuellen Schlüssel eines Piraten zu ermitteln, der den Gruppenschlüssel einer Ebene (das entspricht einer Gruppe von neun Personen) des affinen kopiert und weiterveräußert hat, genügt es, den affinen Raum zu drei diskreten Zeitpunkten derart in neue Ebenen aufzuteilen, daß die Ebenen nicht parallel zueinander verlaufen. Mit anderen Worten, möchte man einen unzuverlässigen Kunden aus den 27 Kunden ermitteln, muß neben den in Fig. 3 und 4 zu unterschiedlichen Zeitpunkten gebildeten Hierarchien noch eine dritte, zu einem dritten Zeitpunkt gebildete Hierarchie erzeugt werden. Werden die drei paarweise nicht parallelen Ebenen, denen jeweils ein bestimmter Gruppenschlüssel zugeordnet ist, miteinander geschnitten, so erhält man einen gemeinsamen Schnittpunkt, der dem unzuverlässigen Kunden entspricht. Die zentrale Stelle muß nur noch veranlassen, daß der zu dem unzuverlässigen Kunden gehörende individuelle kryptografische Schlüssel gesperrt wird.

Noch einfacher wird das Verfahren zur Ermittlung eines unzuverlässigen Kunden durch Schnittmengenbildung, wenn endliche projektive Räume anstelle von endlichen affinen

Räumen verwendet werden, da man hier nicht zwischen parallelen und nichtparallelen Strukturen unterscheiden muß. Die oben beschriebenen Verfahren können auch angewendet werden, wenn ein unzuverlässiger Kunde mehrere individuelle Schlüssel kopiert und diese abwechselnd einsetzt. In diesem Fall müssen aber deutlich mehr Hierarchien zu unterschiedlichen Zeitpunkten gebildet werden. Kennt z.B. ein Pirat zwei von neun individuellen kryptografischen Schlüsseln, so muß die affine Ebene insgesamt dreimal neu in parallele Geraden aufgeteilt werden, um eine fälschliche Identifizierung eines berechtigten Teilnehmers auszuschließen und einen der beiden Schlüssel zu identifizieren.

Anstatt zur Ermittlung des individuellen Schlüssels eines Piraten mehrere Schlüsselhierarchien zu vorbestimmten Zeitpunkten zu bilden müssen, ist es auch vorstellbar, daß verschiedene Schlüsselhierarchien zur gleichen Zeit existieren. In Fig. 5 sind zwei verschiedene Schlüsselhierarchien dargestellt. Mehrere gleichzeitig existierende Schlüsselhierarchien sind sinnvoll, wenn sich mehrere Diensteanbieter eine Kundenchipkarte teilen. Es sei angenommen, daß der Kunde 2 den die beiden Kunden 1 und 2 enthaltenden Gruppenschlüssel 10 des einen Diensteanbieters und den die Kunden 2, 3 und 4 enthaltenden Gruppenschlüssel 20 des anderen Diensteanbieters kopiert und weiterveräußert habe. In diesem Fall kann man den unzuverlässigen Kunden wiederum durch Bildung der Schnittmengen der zugehörigen Gruppen 10 und 20 bestimmen. Wie unter anderem aus Fig. 5 zu erkennen ist, müssen die Teilmengen derselben Hierarchieebene nicht notwendigerweise die gleiche Größe aufweisen.

Patentansprüche

1. Verfahren zum Sichern wenigstens eines durch eine vorbestimmte Hierarchie von kryptografischen Schlüsseln geschützten Systems, insbesondere eines Pay-TV-Systems, gegen unberechtigte Nutzer mit folgenden Verfahrensschritten:
   a) jedem Systemnutzer wird in der untersten Hierarchieebene ein individueller kryptografischer Schlüssel zugeordnet;
   b) die individuellen, kryptografischen Schlüssel werden in einer dem System zugeordneten Speichereinrichtung abgespeichert;
   c) zu vorbestimmten diskreten Zeitpunkten wird wenigstens eine höhere Hierarchieebene von kryptografischen Schlüsseln durch folgende Schritte gebildet:
   - die kryptografischen Schlüssel der unmittelbar niedrigeren Hierarchieebene werden in beliebiger Weise zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt, wobei jeder Teilmenge ein kryptografischer Schlüssel zugeordnet wird, der mit Hilfe der die jeweilige Teilmenge bildenden kryptografischen Schlüssel übertragen und anschließend in der Speichereinrichtung abgelegt wird;
   d) Ermitteln wenigstens eines einem Nutzer zugeordneten individuellen kryptografischen Schlüssels, indem die mengentheoretische Schnittmenge von wenigstens zwei vorbestimmten, zu verschiedenen Zeitpunkten gebildeten Teilmengen, die der gleichen Hierarchieebene angehören, gebildet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Schritte c) und d) ersetzt werden durch die

Schritte:

c') für jedes System werden gleichzeitig wenigstens zwei höhere Hierarchieebene von kryptografischen Schlüsseln durch folgende Schritte gebildet:

- die kryptografischen Schlüssel der unmittelbar niedrigeren Hierarchieebene werden in beliebiger Weise zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt, wobei jeder Teilmenge ein kryptografischer Schlüssel zugeordnet wird, der mit Hilfe der die jeweilige Teilmenge bildenden kryptografischen Schlüssel übertragen und anschließend in der Speichereinrichtung abgelegt wird;

d') Ermitteln wenigstens eines, einem Nutzer zugeordneten individuellen kryptografischen Schlüssels, indem die mengentheoretische Schnittmenge von wenigstens zwei vorbestimmten Teilmengen, die der gleichen Hierarchieebene verschiedener Schlüsselhierarchien angehören, gebildet wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Zusammenfassen der kryptografischen Schlüssel zu Teilmengen vorbestimmter Größe durch endliche geometrische Strukturen festgelegt wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die geometrische Struktur ein endlicher affiner Raum AG(d,q) der Dimension d über dem Körper GF(q) ist.

5. Verfahren zur Ermittlung eines kryptografischen Schlüssels nach Anspruch 3, dadurch gekennzeichnet, daß die geometrische Struktur ein endlicher projektiver Raum PG(d,q) der Dimension d über dem Körper GF(q) ist.

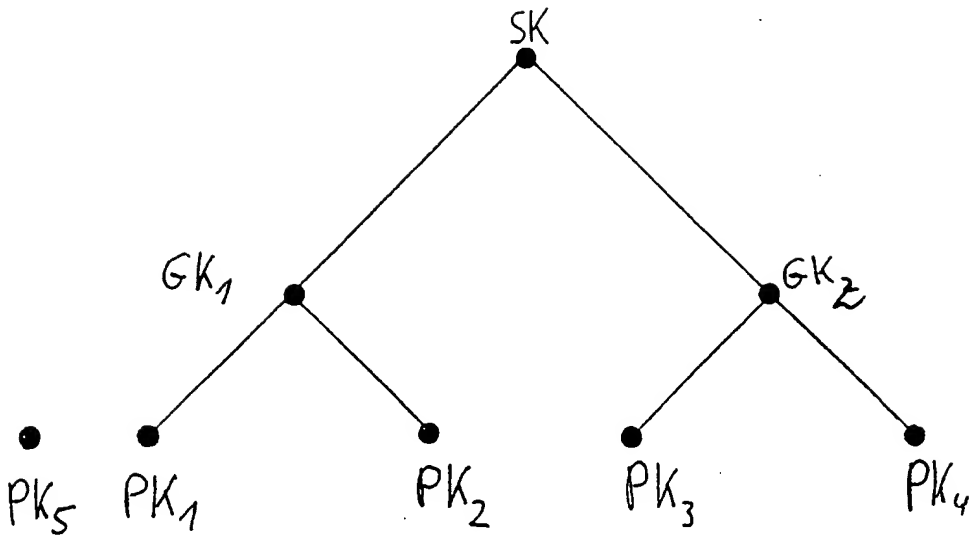


Fig. 1

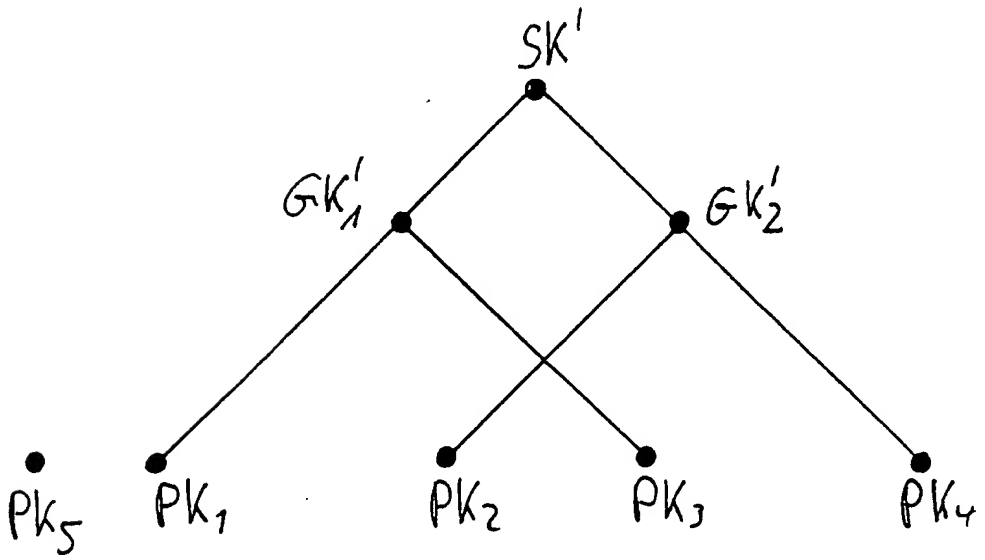


Fig. 2

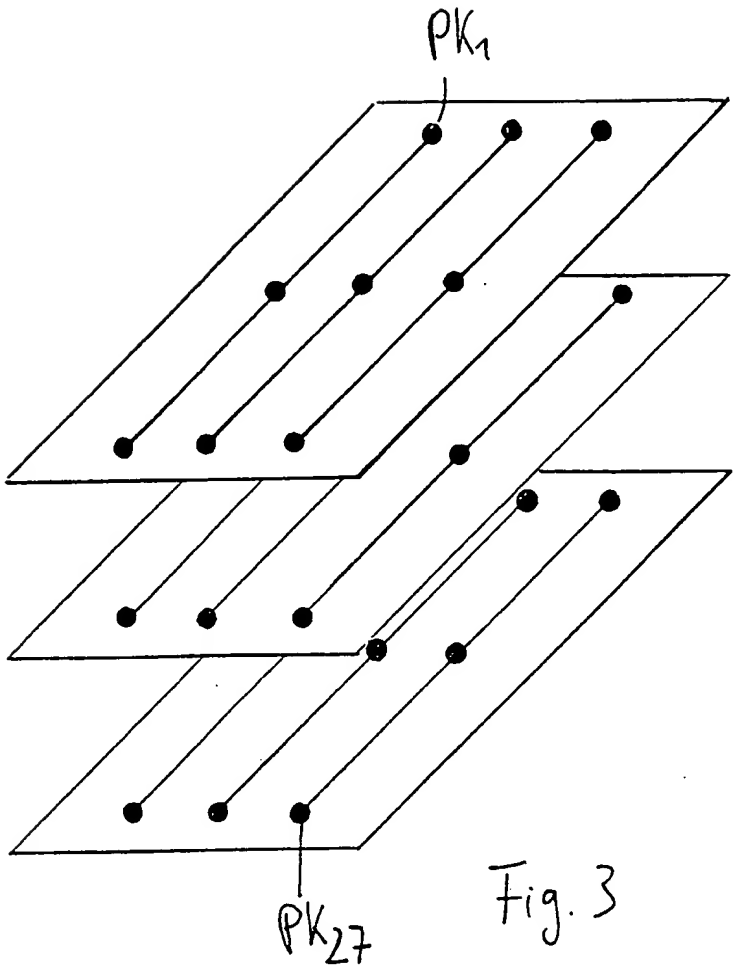


Fig. 3

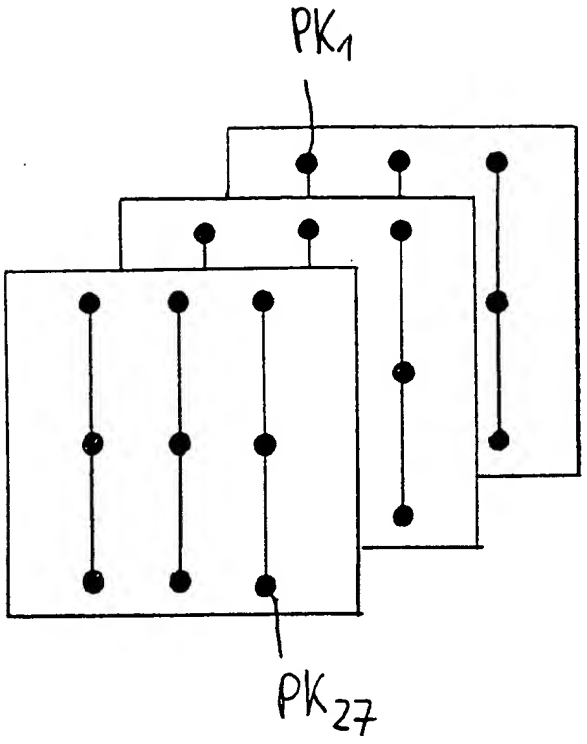


Fig.4

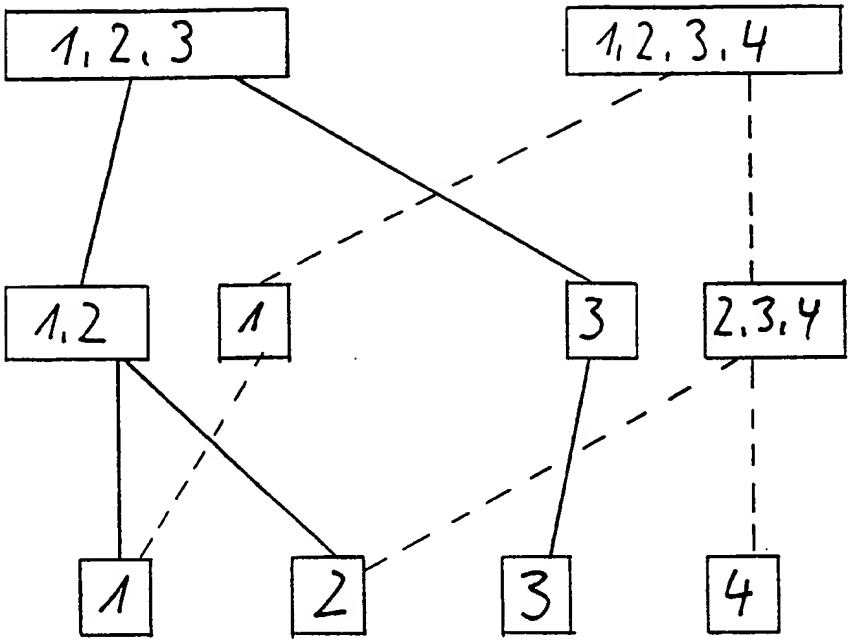


fig. 5

INTERNATIONAL SEARCH REPORT

	ıational Application No
	PCT/EP 97/07124

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/167 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 31 24 150 A (OAK INDUSTRIES INC) 18 March 1982 see page 3, paragraph 1 - paragraph 2 see page 7, paragraph 2 see page 8, paragraph 2 ---	1
A	DE 195 11 298 A (DEUTSCHE TELEKOM AG) 2 October 1996 see column 1, line 57 - column 2, line 22 see column 2, line 61 - column 3, line 37; figure 1 ---	1
A	US 4 771 459 A (JANSEN CORNELIS J A) 13 September 1988 see abstract see column 1, line 46 - column 2, line 16; figures 2-4 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 August 1998	11/08/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fuchs, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 97/07124

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 506 435 A (SCIENTIFIC ATLANTA) 30 September 1992 see abstract see page 8, line 40 - page 9, line 22; figure 7	1
A	LEIN HARN ET AL: "A CRYPTOGRAPHIC KEY GENERATION SCHEME FOR MULTILEVEL DATA SECURITY" 1 October 1990 , COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, VOL. 9, NR. 6, PAGE(S) 539 - 546 XP000162681 see the whole document	1
A	SANTOSH CHOKHANI: "TOWARD A NATINAL PUBLIC KEY INFRASTRUCTURE" IEEE COMMUNICATIONS MAGAZINE, vol. 32, no. 9, 1 September 1994, pages 70-74, XP000476557 cited in the application see the whole document	1

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

I: ational Application No
PCT/EP 97/07124

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3124150 A	18-03-1982	AU 539774 B	18-10-1984
		AU 7187181 A	24-12-1981
		BR 8103848 A	09-03-1982
		CA 1162623 A	21-02-1984
		FR 2485305 A	24-12-1981
		GB 2079109 A,B	10-02-1982
		JP 1455565 C	25-08-1988
		JP 57030438 A	18-02-1982
		JP 63000976 B	09-01-1988
		NL 8102940 A	18-01-1982
		US 4531021 A	23-07-1985
DE 19511298 A	02-10-1996	NONE	
US 4771459 A	13-09-1988	NL 8501211 A	17-11-1986
		EP 0207534 A	07-01-1987
		JP 61252730 A	10-11-1986
EP 0506435 A	30-09-1992	US 5237610 A	17-08-1993
		AT 144670 T	15-11-1996
		AU 650958 B	07-07-1994
		AU 1384092 A	01-10-1992
		CN 1066950 A,B	09-12-1992
		DE 69214698 D	28-11-1996
		DE 69214698 T	06-03-1997
		EP 0679029 A	25-10-1995
		EP 0683614 A	22-11-1995
		JP 5145923 A	11-06-1993
		SG 44801 A	19-12-1997

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 97/07124

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04N7/167 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04N H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 31 24 150 A (OAK INDUSTRIES INC) 18. März 1982 siehe Seite 3, Absatz 1 - Absatz 2 siehe Seite 7, Absatz 2 siehe Seite 8, Absatz 2	1
A	DE 195 11 298 A (DEUTSCHE TELEKOM AG) 2. Oktober 1996 siehe Spalte 1, Zeile 57 - Spalte 2, Zeile 22 siehe Spalte 2, Zeile 61 - Spalte 3, Zeile 37; Abbildung 1	1
A	US 4 771 459 A (JANSEN CORNELIS J A) 13. September 1988 siehe Zusammenfassung siehe Spalte 1, Zeile 46 - Spalte 2, Zeile 16; Abbildungen 2-4	1

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
3. August 1998	11/08/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fuchs, P

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 97/07124

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 506 435 A (SCIENTIFIC ATLANTA) 30. September 1992 siehe Zusammenfassung siehe Seite 8, Zeile 40 - Seite 9, Zeile 22; Abbildung 7	1
A	LEIN HARN ET AL: "A CRYPTOGRAPHIC KEY GENERATION SCHEME FOR MULTILEVEL DATA SECURITY" 1. Oktober 1990 , COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, VOL. 9, NR. 6, PAGE(S) 539 - 546 XP000162681 siehe das ganze Dokument	1
A	SANTOSH CHOKHANI: "TOWARD A NATINAL PUBLIC KEY INFRASTRUCTURE" IEEE COMMUNICATIONS MAGAZINE, Bd. 32, Nr. 9, 1. September 1994, Seiten 70-74, XP000476557 in der Anmeldung erwähnt siehe das ganze Dokument	1

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 97/07124

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 3124150 A	18-03-1982	AU 539774 B	18-10-1984
		AU 7187181 A	24-12-1981
		BR 8103848 A	09-03-1982
		CA 1162623 A	21-02-1984
		FR 2485305 A	24-12-1981
		GB 2079109 A,B	10-02-1982
		JP 1455565 C	25-08-1988
		JP 57030438 A	18-02-1982
		JP 63000976 B	09-01-1988
		NL 8102940 A	18-01-1982
		US 4531021 A	23-07-1985
DE 19511298 A	02-10-1996	KEINE	
US 4771459 A	13-09-1988	NL 8501211 A	17-11-1986
		EP 0207534 A	07-01-1987
		JP 61252730 A	10-11-1986
EP 0506435 A	30-09-1992	US 5237610 A	17-08-1993
		AT 144670 T	15-11-1996
		AU 650958 B	07-07-1994
		AU 1384092 A	01-10-1992
		CN 1066950 A,B	09-12-1992
		DE 69214698 D	28-11-1996
		DE 69214698 T	06-03-1997
		EP 0679029 A	25-10-1995
		EP 0683614 A	22-11-1995
		JP 5145923 A	11-06-1993
		SG 44801 A	19-12-1997